EXHIBIT C-16
EXEMPLARY PORTIONS OF PRIOR ART THAT TEACH OR SUGGEST EACH ELEMENT OF THE ASSERTED '661 CLAIMS
PATENT L.R. 3-3(C)

Claim 1 ('661 Patent)	**U.S. 5,297,201 to Dunlavy ("Dunlavy")**
A cryptographic processing device for securely performing a cryptographic processing operation including a sequence of instructions in a manner resistant to discovery of a secret by external monitoring, comprising:	1:7-12 – "The invention relates to computer security systems and particularly to such a system for preventing remote detection of computer data from computer signal emissions, referred to as Tempest emissions, by generating randomized signal emissions to mask the signal emissions of the computer." 1:15-19 – "Electronic data processing (EDP) equipment such as main-frame computers, minicomputers, personal computers (PCs), word processors and related devices radiate electronic or electromagnetic radio frequency (RF) signals known as Tempest emissions." 2:31-45 – "In a departure from the art, a signal masking technique is employed in which circuitry is coupled to the computer to radiate signals that fully emulate those radiated by the computer to be protected. The emulated signal emissions are synchronized with the computer signal emissions by a special control unit which receives timing instructions from the computer. The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer." 3:20-22 – "In another embodiment for a PC environment, the simulator circuitry is incorporated within the components of a PC." 4:19-44 – "Tempest signal emissions from the EDP 12 and VDU 14 containing decodable data may comprise many types of signals. The signals include carrier and modulation type signals radiated at the fundamental, harmonic and subharmonic frequencies of the clock circuits (not shown) of the EDP 12. Broad band RF signals are also radiated from the EDP 12 by the digital switching of voltage and current levels within the circuitry of the CPU and memory (not shown) during periods when data is being processed, stored or retrieved. Because switching times are relatively short, the spectrum within which this type of radiation takes place is usually limited to frequencies exceeding about 1 MHz. Relatively narrow-band RF

	signals are radiated from the raster circuitry (not shown) of the VDU 14, mostly in the spectrum below about 1 MHz. Broad band RF signals are produced by the video information circuitry (not shown) of the VDU 14, especially those emanating from the modulated high voltage circuits feeding the cathode ray tube (also not shown) of the VDU, in the frequency range of several KHz to over 100 MHz. Additionally, conducted RF signals are produced from electrical currents that flow along remote AC power lines (not shown) connected to the EDP 12, these signals usually being limited to a frequency range lower than a few MHz." 7:33-35 – "FIG. 4 illustrates another embodiment of the present invention comprising a PC 400 which has been modified to prevent remote detection of computer data."
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	4:5-7 – "The EDP 12 includes an input/output (I/O) interface 18 for transferring data to and from the EDP through one or more serial or parallel data ports (not shown)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12." Figure 1.
(b) a source of unpredictable information;	2:40-45 – "The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer." 2:67-3:3 – "A random sequence generator is included as part of the simulator to scramble the sequence of emulated signal emissions, rendering the composite signal meaningless for the purpose of discovering the original data." 3:65-68 – "According to the invention, the signal emission simulator 16 generates randomized signal emissions for the purpose of masking

	the signal emissions of the EDP 12." 4:45-48 – "Referring to FIGS. 1 and 2, the signal emission simulator 16 includes an emulation generator 22, a random sequence generator 24, a broad band RF amplifier 26 and a broad band antenna 28."
(c) a processor:	3:56-57 – "The system 10 includes an electronic data processor (EDP) 12 . . . ." 4:9-13 – "While not shown, it is understood that the EDP 12 includes a central processing unit (CPU), main memory, control and clocking components and other conventional components mounted on an internal printed circuit board (PCB)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12."
(i) connected to said input interface for receiving and cryptographically processing said quantity,	4:5-7 – "The EDP 12 includes an input/output (I/O) interface 18 for transferring data to and from the EDP through one or more serial or parallel data ports (not shown)." 4:9-13 – "While not shown, it is understood that the EDP 12 includes a central processing unit (CPU), main memory, control and clocking components and other conventional components mounted on an internal printed circuit board (PCB)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12."

(ii) configured to use said unpredictable information to conceal a correlation between externally monitorable signals and said secret during said processing of said quantity by modifying said sequence; and	2:40-45 – "The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer." 2:67-3:3 – "A random sequence generator is included as part of the simulator to scramble the sequence of emulated signal emissions, rendering the composite signal meaningless for the purpose of discovering the original data." 3:65-68 – "According to the invention, the signal emission simulator 16 generates randomized signal emissions for the purpose of masking the signal emissions of the EDP 12." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12." 6:29-39 – "Because the modules 34, 36 and 38 of the generator 22 include identical circuit components to those of the EDP 12 and the VDU 14, and because the processing activity of the generator 22 is synchronized with that of the VDU, the simulator 16 produces signal emissions containing substantially the same amplitude and frequency components with respect to time as the signal emissions of the VDU. The amplifier 26 further is utilized to adjust the amplitude components of the simulator signal emissions to match those of the EDP signal emissions." 6:40-53 – "The random sequence generator 24 randomizes the sequence of the signal emissions of the generator 22 so they would be meaningless if decoded. The signals are either randomized or pseudo-randomized. The result is that the simulator 16 produces incoherent signal emissions that overlay or mask the EDP signal emissions to produce composite signal emissions which are not readily decoded. Because the simulated signal emission component is synchronized with the EDP signal emission component, and because the simulated signal emission component is randomized, the resulting composite

	signal emissions are not readily capable of being separated and decoded to recover meaningful data, even with sophisticated equipment."
(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof.	4:5-7 – "The EDP 12 includes an input/output (I/O) interface 18 for transferring data to and from the EDP through one or more serial or parallel data ports (not shown)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12." Figure 1.

Claim 2 ('661 Patent)	**U.S. 5,297,201 to Dunlavy**
The device of claim 1 wherein said input interface and said output interface are the same element.	4:5-7 – "The EDP 12 includes an input/output (I/O) interface 18 for transferring data to and from the EDP through one or more serial or parallel data ports (not shown)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12." Figure 1.

Claim 4 ('661 Patent)	U.S. 5,297,201 to Dunlavy
The device of claim 1 wherein said cryptographic processing operation includes transforming a message with the Data Encryption Standard (DES).	*See, e.g.*, "Data Encryption Standard," Federal Information Processing Standards Publication (FIPS PUB) 46-2, U.S. Department of Commerce, National Institute of Standards and Technology, Dec. 30, 1993 (suggesting, at 3, implementations of DES; and describing, at 5, high level of protection provided by DES); Menezes, A.J. et al., HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC Press, Boca Raton at 223 and 250 (1997)(describing DES as a well known block cipher and a common element of cryptographic systems).

Claim 5 ('661 Patent)	U.S. 5,297,201 to Dunlavy
A cryptographic processing device for securely performing a cryptographic processing operation implementing a permutation in a manner resistant to discovery of a secret by external monitoring, comprising:	1:7-12 – "The invention relates to computer security systems and particularly to such a system for preventing remote detection of computer data from computer signal emissions, referred to as Tempest emissions, by generating randomized signal emissions to mask the signal emissions of the computer." 1:15-19 – "Electronic data processing (EDP) equipment such as main-frame computers, minicomputers, personal computers (PCs), word processors and related devices radiate electronic or electromagnetic radio frequency (RF) signals known as Tempest emissions." 2:31-45 – "In a departure from the art, a signal masking technique is employed in which circuitry is coupled to the computer to radiate signals that fully emulate those radiated by the computer to be protected. The emulated signal emissions are synchronized with the computer signal emissions by a special control unit which receives timing instructions from the computer. The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer." 3:20-22 – "In another embodiment for a PC environment, the simulator circuitry is incorporated within the components of a PC." 4:19-44 – "Tempest signal emissions from the EDP 12 and VDU 14 containing decodable data may comprise many types of signals. The signals include carrier and modulation type signals radiated at the fundamental, harmonic and subharmonic frequencies of the clock circuits (not shown) of the EDP 12. Broad band RF signals are also radiated from the EDP 12 by the digital switching of voltage and

	current levels within the circuitry of the CPU and memory (not shown) during periods when data is being processed, stored or retrieved. Because switching times are relatively short, the spectrum within which this type of radiation takes place is usually limited to frequencies exceeding about 1 MHz. Relatively narrow-band RF signals are radiated from the raster circuitry (not shown) of the VDU 14, mostly in the spectrum below about 1 MHz. Broad band RF signals are produced by the video information circuitry (not shown) of the VDU 14, especially those emanating from the modulated high voltage circuits feeding the cathode ray tube (also not shown) of the VDU, in the frequency range of several KHz to over 100 MHz. Additionally, conducted RF signals are produced from electrical currents that flow along remote AC power lines (not shown) connected to the EDP 12, these signals usually being limited to a frequency range lower than a few MHz." 7:33-35 – "FIG. 4 illustrates another embodiment of the present invention comprising a PC 400 which has been modified to prevent remote detection of computer data." *See also* Menezes, A.J. et al., HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC Press, Boca Raton at 10 (1997)(describing permutations as functions often used in cryptographic constructs); "Data Encryption Standard," Federal Information Processing Standards Publication (FIPS PUB) 46-2, U.S. Department of Commerce, National Institute of Standards and Technology, Dec. 30, 1993 (suggesting, at 3, implementations of DES with microprocessors using ROM, PROM or EEROM; and describing, at 5, high level of protection provided by DES); Menezes, A.J. et al., HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC Press, Boca Raton at 223 and 250 (1997)(describing DES as a well known block cipher and a common element of cryptographic systems).
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	4:5-7 – "The EDP 12 includes an input/output (I/O) interface 18 for transferring data to and from the EDP through one or more serial or parallel data ports (not shown)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34

	generate signal emissions which emulate those of the EDP 12." Figure 1.
(b) a source of unpredictable information;	2:40-45 – "The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer." 2:67-3:3 – "A random sequence generator is included as part of the simulator to scramble the sequence of emulated signal emissions, rendering the composite signal meaningless for the purpose of discovering the original data." 3:65-68 – "According to the invention, the signal emission simulator 16 generates randomized signal emissions for the purpose of masking the signal emissions of the EDP 12." 4:45-48 – "Referring to FIGS. 1 and 2, the signal emission simulator 16 includes an emulation generator 22, a random sequence generator 24, a broad band RF amplifier 26 and a broad band antenna 28."
(c) a processor:	3:56-57 – "The system 10 includes an electronic data processor (EDP) 12 . . . ." 4:9-13 – "While not shown, it is understood that the EDP 12 includes a central processing unit (CPU), main memory, control and clocking components and other conventional components mounted on an internal printed circuit board (PCB)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12."
(i) connected to said input interface for receiving and	4:5-7 – "The EDP 12 includes an input/output (I/O) interface 18 for transferring data to and from the EDP through one or more serial or parallel data ports (not shown)."

cryptographically processing said quantity,	4:9-13 – "While not shown, it is understood that the EDP 12 includes a central processing unit (CPU), main memory, control and clocking components and other conventional components mounted on an internal printed circuit board (PCB)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12."
(ii) configured to use said unpredictable information to conceal a correlation between externally monitorable signals and said secret during said processing of said quantity by randomizing the order of said permutation; and	2:40-45 – "The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer." 2:67-3:3 – "A random sequence generator is included as part of the simulator to scramble the sequence of emulated signal emissions, rendering the composite signal meaningless for the purpose of discovering the original data." 3:65-68 – "According to the invention, the signal emission simulator 16 generates randomized signal emissions for the purpose of masking the signal emissions of the EDP 12." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12." 6:29-39 – "Because the modules 34, 36 and 38 of the generator 22 include identical circuit components to those of the EDP 12 and the

	VDU 14, and because the processing activity of the generator 22 is synchronized with that of the VDU, the simulator 16 produces signal emissions containing substantially the same amplitude and frequency components with respect to time as the signal emissions of the VDU. The amplifier 26 further is utilized to adjust the amplitude components of the simulator signal emissions to match those of the EDP signal emissions." 6:40-53 – "The random sequence generator 24 randomizes the sequence of the signal emissions of the generator 22 so they would be meaningless if decoded. The signals are either randomized or pseudo-randomized. The result is that the simulator 16 produces incoherent signal emissions that overlay or mask the EDP signal emissions to produce composite signal emissions which are not readily decoded. Because the simulated signal emission component is synchronized with the EDP signal emission component, and because the simulated signal emission component is randomized, the resulting composite signal emissions are not readily capable of being separated and decoded to recover meaningful data, even with sophisticated equipment."
(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof.	4:5-7 – "The EDP 12 includes an input/output (I/O) interface 18 for transferring data to and from the EDP through one or more serial or parallel data ports (not shown)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12." Figure 1.

Claim 6 ('661 Patent)	**U.S. 5,297,201 to Dunlavy**
A cryptographic processing device implemented on a single microchip for	1:7-12 – "The invention relates to computer security systems and particularly to such a system for preventing remote detection of computer data from computer signal emissions, referred to as Tempest emissions, by generating randomized signal emissions to mask the

securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring, comprising:	signal emissions of the computer." 1:15-19 – "Electronic data processing (EDP) equipment such as main-frame computers, minicomputers, personal computers (PCs), word processors and related devices radiate electronic or electromagnetic radio frequency (RF) signals known as Tempest emissions." 2:31-45 – "In a departure from the art, a signal masking technique is employed in which circuitry is coupled to the computer to radiate signals that fully emulate those radiated by the computer to be protected. The emulated signal emissions are synchronized with the computer signal emissions by a special control unit which receives timing instructions from the computer. The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer." 3:20-22 – "In another embodiment for a PC environment, the simulator circuitry is incorporated within the components of a PC." 4:19-44 – "Tempest signal emissions from the EDP 12 and VDU 14 containing decodable data may comprise many types of signals. The signals include carrier and modulation type signals radiated at the fundamental, harmonic and subharmonic frequencies of the clock circuits (not shown) of the EDP 12. Broad band RF signals are also radiated from the EDP 12 by the digital switching of voltage and current levels within the circuitry of the CPU and memory (not shown) during periods when data is being processed, stored or retrieved. Because switching times are relatively short, the spectrum within which this type of radiation takes place is usually limited to frequencies exceeding about 1 MHz. Relatively narrow-band RF signals are radiated from the raster circuitry (not shown) of the VDU 14, mostly in the spectrum below about 1 MHz. Broad band RF signals are produced by the video information circuitry (not shown) of the VDU 14, especially those emanating from the modulated high voltage circuits feeding the cathode ray tube (also not shown) of the VDU, in the frequency range of several KHz to over 100 MHz. Additionally, conducted RF signals are produced from electrical currents that flow along remote AC power lines (not shown) connected to the EDP 12, these signals usually being limited to a frequency range lower than a few MHz." 7:33-35 – "FIG. 4 illustrates another embodiment of the present invention comprising a PC 400 which has been modified to prevent

	remote detection of computer data." 8:13-19 – "For example, the invention may be used to prevent signal emission detection from any type of computer, computer peripheral or other type of electronic device. The components of the signal emission simulator may be alternately configured in varying combinations of separate or integrated components, all of which together perform the necessary functions." *See also* Louis C. Guillou and Michel Ugon, "Smart Card, A Highly Reliable and Portable Security Device," Crypto '86 at 471 (1986) (identifies security issue for smart cards: "Absolute physical security does not exist, no more for smart cards than for any other computing device."); Scott Guthery, "Smart Cards," May 28, 1998, www.usenix.org/publications/login/1998-5/guthery.html (visited Dec. 5, 2006) ("Single-chip smart card processors based on these cores are made by almost all the large silicon foundries . . . .Several marketplace forces are at work to open the smart card as a general-purpose computing platform.").
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	4:5-7 – "The EDP 12 includes an input/output (I/O) interface 18 for transferring data to and from the EDP through one or more serial or parallel data ports (not shown)." 4:59-5:4 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12." Figure 1.
(b) a source of unpredictable information;	2:40-45 – "The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer." 2:67-3:3 – "A random sequence generator is included as part of the simulator to scramble the sequence of emulated signal emissions,

	rendering the composite signal meaningless for the purpose of discovering the original data." 3:65-68 – "According to the invention, the signal emission simulator 16 generates randomized signal emissions for the purpose of masking the signal emissions of the EDP 12." 4:45-48 – "Referring to FIGS. 1 and 2, the signal emission simulator 16 includes an emulation generator 22, a random sequence generator 24, a broad band RF amplifier 26 and a broad band antenna 28."
(c) a processor:	3:56-57 – "The system 10 includes an electronic data processor (EDP) 12 . . . ." 4:9-13 – "While not shown, it is understood that the EDP 12 includes a central processing unit (CPU), main memory, control and clocking components and other conventional components mounted on an internal printed circuit board (PCB)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12."
(i) connected to said input interface for receiving and cryptographically processing said quantity,	4:5-7 – "The EDP 12 includes an input/output (I/O) interface 18 for transferring data to and from the EDP through one or more serial or parallel data ports (not shown)." 4:9-13 – "While not shown, it is understood that the EDP 12 includes a central processing unit (CPU), main memory, control and clocking components and other conventional components mounted on an internal printed circuit board (PCB)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed

	circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12."
(ii) configured to use said unpredictable information to conceal a correlation between said microchip's power consumption and said processing of said quantity by expending additional electricity in said microchip during said processing; and	2:40-45 – "The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer." 2:67-3:3 – "A random sequence generator is included as part of the simulator to scramble the sequence of emulated signal emissions, rendering the composite signal meaningless for the purpose of discovering the original data." 3:65-68 – "According to the invention, the signal emission simulator 16 generates randomized signal emissions for the purpose of masking the signal emissions of the EDP 12." 4:34-44 – "Broad band RF signals are produced by the video information circuitry (not shown) of the VDU 14, especially those emanating from the modulated high voltage circuits feeding the cathode ray tube (also not shown) of the VDU, in the frequency range of several KHz to over 100 MHz. Additionally, conducted RF signals are produced from electrical currents that flow along remote AC power lines (not shown) connected to the EDP 12, these signals usually being limited to a frequency range lower than a few MHz." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12." 6:29-39 – "Because the modules 34, 36 and 38 of the generator 22 include identical circuit components to those of the EDP 12 and the VDU 14, and because the processing activity of the generator 22 is synchronized with that of the VDU, the simulator 16 produces signal emissions containing substantially the same amplitude and frequency

	components with respect to time as the signal emissions of the VDU. The amplifier 26 further is utilized to adjust the amplitude components of the simulator signal emissions to match those of the EDP signal emissions." 6:40-53 – "The random sequence generator 24 randomizes the sequence of the signal emissions of the generator 22 so they would be meaningless if decoded. The signals are either randomized or pseudo-randomized. The result is that the simulator 16 produces incoherent signal emissions that overlay or mask the EDP signal emissions to produce composite signal emissions which are not readily decoded. Because the simulated signal emission component is synchronized with the EDP signal emission component, and because the simulated signal emission component is randomized, the resulting composite signal emissions are not readily capable of being separated and decoded to recover meaningful data, even with sophisticated equipment." 7:33-35 – "FIG. 4 illustrates another embodiment of the present invention comprising a PC 400 which has been modified to prevent remote detection of computer data."
(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof.	4:5-7 – "The EDP 12 includes an input/output (I/O) interface 18 for transferring data to and from the EDP through one or more serial or parallel data ports (not shown)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12." Figure 1.

Claim 7 ('661 Patent)	**U.S. 5,297,201 to Dunlavy**
The device of claim 6 including program logic to activate said expending during said	7: 6-19 – "The module 318 is the same as the EDP circuitry module 34 previously described with respect to FIG. 2. The circuitry of the module 318 matches that of the EDP 304, except the module 318 contains a control unit (not shown) similar to the control unit 46 of

processing.	FIG. 2, for synchronizing the processing functions of the module 318 with the processing functions of the EDP 304. The module 320 is the same as the drive circuitry module 38 of FIG. 2 and matches the components of the drive 306. The module 320 includes a hard disk drive 320a and a floppy disk drive 320b. The drive module 320 may be utilized to run a specially-suited computer program (not shown) for performing the randomizing function previously described." *See also* 7:56-61.

Claim 8 ('661 Patent)	**U.S. 5,297,201 to Dunlavy**
The device of claim 7 including (a) program logic implementing said source of unpredictable information; and	7: 6-19 – "The module 318 is the same as the EDP circuitry module 34 previously described with respect to FIG. 2. The circuitry of the module 318 matches that of the EDP 304, except the module 318 contains a control unit (not shown) similar to the control unit 46 of FIG. 2, for synchronizing the processing functions of the module 318 with the processing functions of the EDP 304. The module 320 is the same as the drive circuitry module 38 of FIG. 2 and matches the components of the drive 306. The module 320 includes a hard disk drive 320a and a floppy disk drive 320b. The drive module 320 may be utilized to run a specially-suited computer program (not shown) for performing the randomizing function previously described." *See also* 7:56-61.
(b) program logic to transmit said unpredictable information to an additional power expending circuit contained in said microchip.	5:62-6:9 – "The random sequence generator 24 of the simulator 16 is connected to the generator 22 by a line 52. The generator 24 convolutes or 'scrambles' the sequence of the signals generated by the generator 22, so that they would be meaningless if decoded. This is important since the generator 22 has just generated synchronous signals with the same character signatures as the EDP 12. The random sequence generator 24 comprises a circuit that operates as a noise source for introducing random or pseudo-random noise signals to the signals produced by the generator 22. The resulting signals are thereby convoluted in sequence, time, frequency and/or amplitude and thus garble any data that might have been decodable from the signals. The generator 24 comprises a random sequence generator circuit." 6:11-18 – "Alternatively, the generator 24 comprises a specially-written computer program contained on a suitably shielded storage medium such as a hard disk or continuous tape, which is then run on the drive circuitry 38. The program may also be stored in the ROM BIOS (not shown) of the generator 22. Such a program must also produce the equivalent of a random or psuedo-random [sic] digital

	sequence in order to be effective." 6:29-39 – "Because the modules 34, 36 and 38 of the generator 22 include identical circuit components to those of the EDP 12 and the VDU 14, and because the processing activity of the generator 22 is synchronized with that of the VDU, the simulator 16 produces signal emissions containing substantially the same amplitude and frequency components with respect to time as the signal emissions of the VDU. The amplifier 26 further is utilized to adjust the amplitude components of the simulator signal emissions to match those of the EDP signal emissions." 7: 6-19 – "The module 318 is the same as the EDP circuitry module 34 previously described with respect to FIG. 2. The circuitry of the module 318 matches that of the EDP 304, except the module 318 contains a control unit (not shown) similar to the control unit 46 of FIG. 2, for synchronizing the processing functions of the module 318 with the processing functions of the EDP 304. The module 320 is the same as the drive circuitry module 38 of FIG. 2 and matches the components of the drive 306. The module 320 includes a hard disk drive 320a and a floppy disk drive 320b. The drive module 320 may be utilized to run a specially-suited computer program (not shown) for performing the randomizing function previously described." *See also* 7:56-61. Figure 1.

Claim 9 ('661 Patent)	**U.S. 5,297,201 to Dunlavy**
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring, comprising:	1:7-12 – "The invention relates to computer security systems and particularly to such a system for preventing remote detection of computer data from computer signal emissions, referred to as Tempest emissions, by generating randomized signal emissions to mask the signal emissions of the computer." 1:15-19 – "Electronic data processing (EDP) equipment such as main-frame computers, minicomputers, personal computers (PCs), word processors and related devices radiate electronic or electromagnetic radio frequency (RF) signals known as Tempest emissions." 2:31-45 – "In a departure from the art, a signal masking technique is employed in which circuitry is coupled to the computer to radiate signals that fully emulate those radiated by the computer to be protected. The emulated signal emissions are synchronized with the computer signal emissions by a special control unit which receives

	timing instructions from the computer. The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer." 3:20-22 – "In another embodiment for a PC environment, the simulator circuitry is incorporated within the components of a PC." 4:19-44 – "Tempest signal emissions from the EDP 12 and VDU 14 containing decodable data may comprise many types of signals. The signals include carrier and modulation type signals radiated at the fundamental, harmonic and subharmonic frequencies of the clock circuits (not shown) of the EDP 12. Broad band RF signals are also radiated from the EDP 12 by the digital switching of voltage and current levels within the circuitry of the CPU and memory (not shown) during periods when data is being processed, stored or retrieved. Because switching times are relatively short, the spectrum within which this type of radiation takes place is usually limited to frequencies exceeding about 1 MHz. Relatively narrow-band RF signals are radiated from the raster circuitry (not shown) of the VDU 14, mostly in the spectrum below about 1 MHz. Broad band RF signals are produced by the video information circuitry (not shown) of the VDU 14, especially those emanating from the modulated high voltage circuits feeding the cathode ray tube (also not shown) of the VDU, in the frequency range of several KHz to over 100 MHz. Additionally, conducted RF signals are produced from electrical currents that flow along remote AC power lines (not shown) connected to the EDP 12, these signals usually being limited to a frequency range lower than a few MHz." 7:33-35 – "FIG. 4 illustrates another embodiment of the present invention comprising a PC 400 which has been modified to prevent remote detection of computer data." 8:13-19 – "For example, the invention may be used to prevent signal emission detection from any type of computer, computer peripheral or other type of electronic device. The components of the signal emission simulator may be alternately configured in varying combinations of separate or integrated components, all of which together perform the necessary functions."
(a) an input interface for receiving a quantity to be cryptographically	4:5-7 – "The EDP 12 includes an input/output (I/O) interface 18 for transferring data to and from the EDP through one or more serial or parallel data ports (not shown)."

processed, said quantity being representative of at least a portion of a message;	4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12." Figure 1.
(b) a source of unpredictable information;	2:40-45 – "The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer." 2:67-3:3 – "A random sequence generator is included as part of the simulator to scramble the sequence of emulated signal emissions, rendering the composite signal meaningless for the purpose of discovering the original data." 3:65-68 – "According to the invention, the signal emission simulator 16 generates randomized signal emissions for the purpose of masking the signal emissions of the EDP 12." 4:45-48 – "Referring to FIGS. 1 and 2, the signal emission simulator 16 includes an emulation generator 22, a random sequence generator 24, a broad band RF amplifier 26 and a broad band antenna 28."
(c) a processor:	3:56-57 – "The system 10 includes an electronic data processor (EDP) 12 . . . ." 4:9-13 – "While not shown, it is understood that the EDP 12 includes a central processing unit (CPU), main memory, control and clocking components and other conventional components mounted on an internal printed circuit board (PCB)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38.

	Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12."
(i) connected to said input interface for receiving and cryptographically processing said quantity,	4:5-7 – "The EDP 12 includes an input/output (I/O) interface 18 for transferring data to and from the EDP through one or more serial or parallel data ports (not shown)." 4:9-13 – "While not shown, it is understood that the EDP 12 includes a central processing unit (CPU), main memory, control and clocking components and other conventional components mounted on an internal printed circuit board (PCB)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12."
(ii) configured to use said unpredictable information to conceal a correlation between externally monitorable signals and said secret during said processing of said quantity;	2:40-45 – "The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer." 2:67-3:3 – "A random sequence generator is included as part of the simulator to scramble the sequence of emulated signal emissions, rendering the composite signal meaningless for the purpose of discovering the original data." 3:65-68 – "According to the invention, the signal emission simulator 16 generates randomized signal emissions for the purpose of masking the signal emissions of the EDP 12." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be

	protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12." 6:29-39 – "Because the modules 34, 36 and 38 of the generator 22 include identical circuit components to those of the EDP 12 and the VDU 14, and because the processing activity of the generator 22 is synchronized with that of the VDU, the simulator 16 produces signal emissions containing substantially the same amplitude and frequency components with respect to time as the signal emissions of the VDU. The amplifier 26 further is utilized to adjust the amplitude components of the simulator signal emissions to match those of the EDP signal emissions." 6:40-53 – "The random sequence generator 24 randomizes the sequence of the signal emissions of the generator 22 so they would be meaningless if decoded. The signals are either randomized or pseudo-randomized. The result is that the simulator 16 produces incoherent signal emissions that overlay or mask the EDP signal emissions to produce composite signal emissions which are not readily decoded. Because the simulated signal emission component is synchronized with the EDP signal emission component, and because the simulated signal emission component is randomized, the resulting composite signal emissions are not readily capable of being separated and decoded to recover meaningful data, even with sophisticated equipment." 7:33-35 – "FIG. 4 illustrates another embodiment of the present invention comprising a PC 400 which has been modified to prevent remote detection of computer data."
(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof;	4:5-7 – "The EDP 12 includes an input/output (I/O) interface 18 for transferring data to and from the EDP through one or more serial or parallel data ports (not shown)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed

	circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12." Figure 1.
(e) a hardware-implemented noise production subunit connected to said source of unpredictable information and configured to expend unpredictable amounts of electricity based on the output of said source of unpredictable information; and	2:67-3:3 – "A random sequence generator is included as part of the simulator to scramble the sequence of emulated signal emissions, rendering the composite signal meaningless for the purpose of discovering the original data." 3:65-68 – "According to the invention, the signal emission simulator 16 generates randomized signal emissions for the purpose of masking the signal emissions of the EDP 12." 4:45-48 – "Referring to FIGS. 1 and 2, the signal emission simulator 16 includes an emulation generator 22, a random sequence generator 24, a broad band RF amplifier 26 and a broad band antenna 28." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12." 6:29-39 – "Because the modules 34, 36 and 38 of the generator 22 include identical circuit components to those of the EDP 12 and the VDU 14, and because the processing activity of the generator 22 is synchronized with that of the VDU, the simulator 16 produces signal emissions containing substantially the same amplitude and frequency components with respect to time as the signal emissions of the VDU. The amplifier 26 further is utilized to adjust the amplitude components of the simulator signal emissions to match those of the EDP signal emissions." 6:40-53 – "The random sequence generator 24 randomizes the sequence of the signal emissions of the generator 22 so they would be meaningless if decoded. The signals are either randomized or pseudo-randomized. The result is that the simulator 16 produces incoherent signal emissions that overlay or mask the EDP signal emissions to

	produce composite signal emissions which are not readily decoded. Because the simulated signal emission component is synchronized with the EDP signal emission component, and because the simulated signal emission component is randomized, the resulting composite signal emissions are not readily capable of being separated and decoded to recover meaningful data, even with sophisticated equipment." 7: 6-19 – "The module 318 is the same as the EDP circuitry module 34 previously described with respect to FIG. 2. The circuitry of the module 318 matches that of the EDP 304, except the module 318 contains a control unit (not shown) similar to the control unit 46 of FIG. 2, for synchronizing the processing functions of the module 318 with the processing functions of the EDP 304. The module 320 is the same as the drive circuitry module 38 of FIG. 2 and matches the components of the drive 306. The module 320 includes a hard disk drive 320a and a floppy disk drive 320b. The drive module 320 may be utilized to run a specially-suited computer program (not shown) for performing the randomizing function previously described."
(f) an activation controller, which may be activated by software contained in said device, to activate and deactivate said expending of unpredictable amounts of electricity.	6:11-18 – "Alternatively, the generator 24 comprises a specially-written computer program contained on a suitably shielded storage medium such as a hard disk or continuous tape, which is then run on the drive circuitry 38. The program may also be stored in the ROM BIOS (not shown) of the generator 22. Such a program must also produce the equivalent of a random or psuedo-random [sic] digital sequence in order to be effective." 7: 6-19 – "The module 318 is the same as the EDP circuitry module 34 previously described with respect to FIG. 2. The circuitry of the module 318 matches that of the EDP 304, except the module 318 contains a control unit (not shown) similar to the control unit 46 of FIG. 2, for synchronizing the processing functions of the module 318 with the processing functions of the EDP 304. The module 320 is the same as the drive circuitry module 38 of FIG. 2 and matches the components of the drive 306. The module 320 includes a hard disk drive 320a and a floppy disk drive 320b. The drive module 320 may be utilized to run a specially-suited computer program (not shown) for performing the randomizing function previously described." *See also* 7:56-61. Figure 1.

Claim 10 ('661 Patent)	U.S. 5,297,201 to Dunlavy
The device of claim 9 wherein said source of unpredictable information is a hardware-implemented random number generator, and wherein said noise production subunit includes a digital-to-analog converter.	4:53-62 – "As discussed below, the simulator 16 generates signal emissions to mask those of the EDP 12 and VDU 14. The generated signal emissions are synchronized to those of the EDP 12 with respect to amplitude, time and frequency, and then are randomized in their sequence. The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection." 6:8-10 – "The generator 24 comprises a random sequence generator circuit. Since such a circuit is familiar to those skilled in the art, it is not described further." 8:23-27 – "Also, the emulated signal emissions may be synchronized with the signal emissions of the computer with respect to one or any combination of time, frequency and amplitude parameters." Claim 5 – "The apparatus of claim 1 wherein said generated signal emissions are synchronized with said data processor signal emissions with respect to amplitude." Claim 11 – "The apparatus of claim 9 wherein said generated signal emissions are synchronized with said data processor signal emissions with respect to at least one of time, frequency and amplitude." *See also, e.g.,* English abstracts of JP10084223, JP10197610, JP62260406, and JP62082702 (describing including a digital to analog converter in a noise production subunit); U.S. Patent No. 5,157,725 to Lindholm at, *e.g.*, 5:32-44 (disclosing random number generator for generating bit signal sequences).

Claim 11 ('661 Patent)	U.S. 5,297,201 to Dunlavy
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external measurement of said device's power consumption,	1:7-12 – "The invention relates to computer security systems and particularly to such a system for preventing remote detection of computer data from computer signal emissions, referred to as Tempest emissions, by generating randomized signal emissions to mask the signal emissions of the computer." 1: 15-19 – "Electronic data processing (EDP) equipment such as main-frame computers, minicomputers, personal computers (PCs), word processors and related devices radiate electronic or electromagnetic radio frequency (RF) signals known as Tempest

comprising:	emissions." 2:31-45 – "In a departure from the art, a signal masking technique is employed in which circuitry is coupled to the computer to radiate signals that fully emulate those radiated by the computer to be protected. The emulated signal emissions are synchronized with the computer signal emissions by a special control unit which receives timing instructions from the computer. The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer." 3:20-22 – "In another embodiment for a PC environment, the simulator circuitry is incorporated within the components of a PC." 4:19-44 – "Tempest signal emissions from the EDP 12 and VDU 14 containing decodable data may comprise many types of signals. The signals include carrier and modulation type signals radiated at the fundamental, harmonic and subharmonic frequencies of the clock circuits (not shown) of the EDP 12. Broad band RF signals are also radiated from the EDP 12 by the digital switching of voltage and current levels within the circuitry of the CPU and memory (not shown) during periods when data is being processed, stored or retrieved. Because switching times are relatively short, the spectrum within which this type of radiation takes place is usually limited to frequencies exceeding about 1 MHz. Relatively narrow-band RF signals are radiated from the raster circuitry (not shown) of the VDU 14, mostly in the spectrum below about 1 MHz. Broad band RF signals are produced by the video information circuitry (not shown) of the VDU 14, especially those emanating from the modulated high voltage circuits feeding the cathode ray tube (also not shown) of the VDU, in the frequency range of several KHz to over 100 MHz. Additionally, conducted RF signals are produced from electrical currents that flow along remote AC power lines (not shown) connected to the EDP 12, these signals usually being limited to a frequency range lower than a few MHz." 7:33-35 – "FIG. 4 illustrates another embodiment of the present invention comprising a PC 400 which has been modified to prevent remote detection of computer data."
(a) an input interface for receiving a quantity to be cryptographically	4:5-7 – "The EDP 12 includes an input/output (I/O) interface 18 for transferring data to and from the EDP through one or more serial or parallel data ports (not shown)."

processed, said quantity being representative of at least a portion of a message;	4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12." Figure 1.
(b) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	1:45-58 – "One method used to protect computer data is to employ electromagnetic shielding which reduces the level of the signal emissions emanating from the computer, thus preventing effective reception at reasonable distances." 4:34-44 – "Broad band RF signals are produced by the video information circuitry (not shown) of the VDU 14, especially those emanating from the modulated high voltage circuits feeding the cathode ray tube (also not shown) of the VDU, in the frequency range of several KHz to over 100 MHz. Additionally, conducted RF signals are produced from electrical currents that flow along remote AC power lines (not shown) connected to the EDP 12, these signals usually being limited to a frequency range lower than a few MHz."
(c) a processor connected to said input interface for receiving and cryptographically processing said quantity; and	3:56-57 – "The system 10 includes an electronic data processor (EDP) 12 . . . ." 4:5-7 – "The EDP 12 includes an input/output (I/O) interface 18 for transferring data to and from the EDP through one or more serial or parallel data ports (not shown)." 4:9-13 – "While not shown, it is understood that the EDP 12 includes a central processing unit (CPU), main memory, control and clocking components and other conventional components mounted on an internal printed circuit board (PCB)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed

	circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12."
(d) a noise production system for introducing noise into said measurement of said power consumption.	2:31-45 – "In a departure from the art, a signal masking technique is employed in which circuitry is coupled to the computer to radiate signals that fully emulate those radiated by the computer to be protected. The emulated signal emissions are synchronized with the computer signal emissions by a special control unit which receives timing instructions from the computer. The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer." 2:67-3:3 – "A random sequence generator is included as part of the simulator to scramble the sequence of emulated signal emissions, rendering the composite signal meaningless for the purpose of discovering the original data." 3:65-68 – "According to the invention, the signal emission simulator 16 generates randomized signal emissions for the purpose of masking the signal emissions of the EDP 12." 4:34-44 – "Broad band RF signals are produced by the video information circuitry (not shown) of the VDU 14, especially those emanating from the modulated high voltage circuits feeding the cathode ray tube (also not shown) of the VDU, in the frequency range of several KHz to over 100 MHz. Additionally, conducted RF signals are produced from electrical currents that flow along remote AC power lines (not shown) connected to the EDP 12, these signals usually being limited to a frequency range lower than a few MHz." 4:45-48 – "Referring to FIGS. 1 and 2, the signal emission simulator 16 includes an emulation generator 22, a random sequence generator 24, a broad band RF amplifier 26 and a broad band antenna 28." 5:49-61 – "The amplifier 32 and antenna 28 in combination provide additional signal amplitude to the signal emissions of the generator 22." 5:62-6:7 – "The random sequence generator 24 of the simulator 16 is connected to the generator 22 by a line 52. The generator 24 convolutes or 'scrambles' the sequence of the signals generated by the generator 22, so that they would be meaningless if decoded. This is

	important since the generator 22 has just generated synchronous signals with the same character signatures as the EDP 12. The random sequence generator 24 comprises a circuit that operates as a noise source for introducing random or pseudo-random noise signals to the signals produced by the generator 22. The resulting signals are thereby convoluted in sequence, time, frequency and/or amplitude and thus garble any data that might have been decodable from the signals." 6:8-9 – "The generator 24 comprises a random sequence generator circuit." 7:33-35 – "FIG. 4 illustrates another embodiment of the present invention comprising a PC 400 which has been modified to prevent remote detection of computer data." Figure 1.

Claim 22 ('661 Patent)	**U.S. 5,297,201 to Dunlavy**
A device according to claims 1, 4, 7, 9, 11, 14, 15, or 20 wherein said device comprises a smartcard.	8:13-19 – "For example, the invention may be used to prevent signal emission detection from any type of computer, computer peripheral or other type of electronic device. The components of the signal emission simulator may be alternately configured in varying combinations of separate or integrated components, all of which together perform the necessary functions." *See also* Scott Guthery, "Smart Cards," May 28, 1998, www.usenix.org/publications/login/1998-5/guthery.html (visited Dec. 5, 2006) ("Several marketplace forces are at work to open the smart card as a general-purpose computing platform.").

Claim 27 ('661 Patent)	**U.S. 5,297,201 to Dunlavy**
A method of securely performing a cryptographic processing operation including a sequence of instructions in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring,	1:7-12 – "The invention relates to computer security systems and particularly to such a system for preventing remote detection of computer data from computer signal emissions, referred to as Tempest emissions, by generating randomized signal emissions to mask the signal emissions of the computer." 1:15-19 – "Electronic data processing (EDP) equipment such as main-frame computers, minicomputers, personal computers (PCs), word processors and related devices radiate electronic or electromagnetic radio frequency (RF) signals known as Tempest emissions."

comprising:	2:31-45 – "In a departure from the art, a signal masking technique is employed in which circuitry is coupled to the computer to radiate signals that fully emulate those radiated by the computer to be protected. The emulated signal emissions are synchronized with the computer signal emissions by a special control unit which receives timing instructions from the computer. The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer." 3:20-22 – "In another embodiment for a PC environment, the simulator circuitry is incorporated within the components of a PC." 4:19-44 – "Tempest signal emissions from the EDP 12 and VDU 14 containing decodable data may comprise many types of signals. The signals include carrier and modulation type signals radiated at the fundamental, harmonic and subharmonic frequencies of the clock circuits (not shown) of the EDP 12. Broad band RF signals are also radiated from the EDP 12 by the digital switching of voltage and current levels within the circuitry of the CPU and memory (not shown) during periods when data is being processed, stored or retrieved. Because switching times are relatively short, the spectrum within which this type of radiation takes place is usually limited to frequencies exceeding about 1 MHz. Relatively narrow-band RF signals are radiated from the raster circuitry (not shown) of the VDU 14, mostly in the spectrum below about 1 MHz. Broad band RF signals are produced by the video information circuitry (not shown) of the VDU 14, especially those emanating from the modulated high voltage circuits feeding the cathode ray tube (also not shown) of the VDU, in the frequency range of several KHz to over 100 MHz. Additionally, conducted RF signals are produced from electrical currents that flow along remote AC power lines (not shown) connected to the EDP 12, these signals usually being limited to a frequency range lower than a few MHz." 7:33-35 – "FIG. 4 illustrates another embodiment of the present invention comprising a PC 400 which has been modified to prevent remote detection of computer data."
(a) receiving a quantity to be cryptographically processed, said quantity being representative of at	4:5-7 – "The EDP 12 includes an input/output (I/O) interface 18 for transferring data to and from the EDP through one or more serial or parallel data ports (not shown)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for

least a portion of a message;	processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12." Figure 1.
(b) generating unpredictable information;	2:40-45 – "The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer." 2:67-3:3 – "A random sequence generator is included as part of the simulator to scramble the sequence of emulated signal emissions, rendering the composite signal meaningless for the purpose of discovering the original data." 3:65-68 – "According to the invention, the signal emission simulator 16 generates randomized signal emissions for the purpose of masking the signal emissions of the EDP 12." 4:45-48 – "Referring to FIGS. 1 and 2, the signal emission simulator 16 includes an emulation generator 22, a random sequence generator 24, a broad band RF amplifier 26 and a broad band antenna 28."
(c) using said unpredictable information while processing said quantity to conceal a correlation between externally monitorable signals and said secret by using said unpredictable information to modify said sequence; and	2:40-45 – "The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer." 2:67-3:3 – "A random sequence generator is included as part of the simulator to scramble the sequence of emulated signal emissions, rendering the composite signal meaningless for the purpose of discovering the original data." 3:65-68 – "According to the invention, the signal emission simulator 16 generates randomized signal emissions for the purpose of masking

	the signal emissions of the EDP 12." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12." 6:29-39 – "Because the modules 34, 36 and 38 of the generator 22 include identical circuit components to those of the EDP 12 and the VDU 14, and because the processing activity of the generator 22 is synchronized with that of the VDU, the simulator 16 produces signal emissions containing substantially the same amplitude and frequency components with respect to time as the signal emissions of the VDU. The amplifier 26 further is utilized to adjust the amplitude components of the simulator signal emissions to match those of the EDP signal emissions." 6:40-53 – "The random sequence generator 24 randomizes the sequence of the signal emissions of the generator 22 so they would be meaningless if decoded. The signals are either randomized or pseudo-randomized. The result is that the simulator 16 produces incoherent signal emissions that overlay or mask the EDP signal emissions to produce composite signal emissions which are not readily decoded. Because the simulated signal emission component is synchronized with the EDP signal emission component, and because the simulated signal emission component is randomized, the resulting composite signal emissions are not readily capable of being separated and decoded to recover meaningful data, even with sophisticated equipment." 7:33-35 – "FIG. 4 illustrates another embodiment of the present invention comprising a PC 400 which has been modified to prevent remote detection of computer data."
(d) outputting said cryptographically processed quantity to a recipient thereof.	4:5-7 – "The EDP 12 includes an input/output (I/O) interface 18 for transferring data to and from the EDP through one or more serial or parallel data ports (not shown)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for

	processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12." Figure 1.

Claim 28 ('661 Patent)	**U.S. 5,297,201 to Dunlavy**
A method of securely performing a cryptographic processing operation implementing a permutation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring, comprising:	1:7-12 – "The invention relates to computer security systems and particularly to such a system for preventing remote detection of computer data from computer signal emissions, referred to as Tempest emissions, by generating randomized signal emissions to mask the signal emissions of the computer." 1:15-19 – "Electronic data processing (EDP) equipment such as main-frame computers, minicomputers, personal computers (PCs), word processors and related devices radiate electronic or electromagnetic radio frequency (RF) signals known as Tempest emissions." 2:31-45 – "In a departure from the art, a signal masking technique is employed in which circuitry is coupled to the computer to radiate signals that fully emulate those radiated by the computer to be protected. The emulated signal emissions are synchronized with the computer signal emissions by a special control unit which receives timing instructions from the computer. The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer." 3:20-22 – "In another embodiment for a PC environment, the simulator circuitry is incorporated within the components of a PC." 4:19-44 – "Tempest signal emissions from the EDP 12 and VDU 14 containing decodable data may comprise many types of signals. The signals include carrier and modulation type signals radiated at the fundamental, harmonic and subharmonic frequencies of the clock circuits (not shown) of the EDP 12. Broad band RF signals are also

	radiated from the EDP 12 by the digital switching of voltage and current levels within the circuitry of the CPU and memory (not shown) during periods when data is being processed, stored or retrieved. Because switching times are relatively short, the spectrum within which this type of radiation takes place is usually limited to frequencies exceeding about 1 MHz. Relatively narrow-band RF signals are radiated from the raster circuitry (not shown) of the VDU 14, mostly in the spectrum below about 1 MHz. Broad band RF signals are produced by the video information circuitry (not shown) of the VDU 14, especially those emanating from the modulated high voltage circuits feeding the cathode ray tube (also not shown) of the VDU, in the frequency range of several KHz to over 100 MHz. Additionally, conducted RF signals are produced from electrical currents that flow along remote AC power lines (not shown) connected to the EDP 12, these signals usually being limited to a frequency range lower than a few MHz." 7:33-35 – "FIG. 4 illustrates another embodiment of the present invention comprising a PC 400 which has been modified to prevent remote detection of computer data." *See also* Menezes, A.J. et al., HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC Press, Boca Raton at 10 (1997)(describing permutations as functions often used in cryptographic constructs); "Data Encryption Standard," Federal Information Processing Standards Publication (FIPS PUB) 46-2, U.S. Department of Commerce, National Institute of Standards and Technology, Dec. 30, 1993 (suggesting, at 3, implementations of DES with microprocessors using ROM, PROM or EEROM; and describing, at 5, high level of protection provided by DES); Menezes, A.J. et al., HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC Press, Boca Raton at 223 and 250 (1997)(describing DES as a well known block cipher and a common element of cryptographic systems).
(a) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	4:5-7 – "The EDP 12 includes an input/output (I/O) interface 18 for transferring data to and from the EDP through one or more serial or parallel data ports (not shown)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a

	central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12." Figure 1.
(b) generating unpredictable information;	2:40-45 – "The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer." 2:67-3:3 – "A random sequence generator is included as part of the simulator to scramble the sequence of emulated signal emissions, rendering the composite signal meaningless for the purpose of discovering the original data." 3:65-68 – "According to the invention, the signal emission simulator 16 generates randomized signal emissions for the purpose of masking the signal emissions of the EDP 12." 4:45-48 – "Referring to FIGS. 1 and 2, the signal emission simulator 16 includes an emulation generator 22, a random sequence generator 24, a broad band RF amplifier 26 and a broad band antenna 28."
(c) using said unpredictable information while processing said quantity to conceal a correlation between externally monitorable signals and said secret by randomizing the order of said permutation; and	2:40-45 – "The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer." 2:67-3:3 – "A random sequence generator is included as part of the simulator to scramble the sequence of emulated signal emissions, rendering the composite signal meaningless for the purpose of discovering the original data." 3:65-68 – "According to the invention, the signal emission simulator 16 generates randomized signal emissions for the purpose of masking the signal emissions of the EDP 12." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the

	module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12." 6:29-39 – "Because the modules 34, 36 and 38 of the generator 22 include identical circuit components to those of the EDP 12 and the VDU 14, and because the processing activity of the generator 22 is synchronized with that of the VDU, the simulator 16 produces signal emissions containing substantially the same amplitude and frequency components with respect to time as the signal emissions of the VDU. The amplifier 26 further is utilized to adjust the amplitude components of the simulator signal emissions to match those of the EDP signal emissions." 6:40-53 – "The random sequence generator 24 randomizes the sequence of the signal emissions of the generator 22 so they would be meaningless if decoded. The signals are either randomized or pseudo-randomized. The result is that the simulator 16 produces incoherent signal emissions that overlay or mask the EDP signal emissions to produce composite signal emissions which are not readily decoded. Because the simulated signal emission component is synchronized with the EDP signal emission component, and because the simulated signal emission component is randomized, the resulting composite signal emissions are not readily capable of being separated and decoded to recover meaningful data, even with sophisticated equipment." 7:33-35 – "FIG. 4 illustrates another embodiment of the present invention comprising a PC 400 which has been modified to prevent remote detection of computer data."
(d) outputting said cryptographically processed quantity to a recipient thereof.	4:5-7 – "The EDP 12 includes an input/output (I/O) interface 18 for transferring data to and from the EDP through one or more serial or parallel data ports (not shown)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34

	generate signal emissions which emulate those of the EDP 12." Figure 1.

Claim 29 ('661 Patent)	U.S. 5,297,201 to Dunlavy
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of said device's power consumption, comprising:	1:7-12 – "The invention relates to computer security systems and particularly to such a system for preventing remote detection of computer data from computer signal emissions, referred to as Tempest emissions, by generating randomized signal emissions to mask the signal emissions of the computer." 1:15-19 – "Electronic data processing (EDP) equipment such as main-frame computers, minicomputers, personal computers (PCs), word processors and related devices radiate electronic or electromagnetic radio frequency (RF) signals known as Tempest emissions." 2:31-45 – "In a departure from the art, a signal masking technique is employed in which circuitry is coupled to the computer to radiate signals that fully emulate those radiated by the computer to be protected. The emulated signal emissions are synchronized with the computer signal emissions by a special control unit which receives timing instructions from the computer. The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer." 3:20-22 – "In another embodiment for a PC environment, the simulator circuitry is incorporated within the components of a PC." 4:19-44 – "Tempest signal emissions from the EDP 12 and VDU 14 containing decodable data may comprise many types of signals. The signals include carrier and modulation type signals radiated at the fundamental, harmonic and subharmonic frequencies of the clock circuits (not shown) of the EDP 12. Broad band RF signals are also radiated from the EDP 12 by the digital switching of voltage and current levels within the circuitry of the CPU and memory (not shown) during periods when data is being processed, stored or retrieved. Because switching times are relatively short, the spectrum within which this type of radiation takes place is usually limited to frequencies exceeding about 1 MHz. Relatively narrow-band RF signals are radiated from the raster circuitry (not shown) of the VDU 14, mostly in the spectrum below about 1 MHz. Broad band RF

	signals are produced by the video information circuitry (not shown) of the VDU 14, especially those emanating from the modulated high voltage circuits feeding the cathode ray tube (also not shown) of the VDU, in the frequency range of several KHz to over 100 MHz. Additionally, conducted RF signals are produced from electrical currents that flow along remote AC power lines (not shown) connected to the EDP 12, these signals usually being limited to a frequency range lower than a few MHz."
(a) receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	1:45-58 – "One method used to protect computer data is to employ electromagnetic shielding which reduces the level of the signal emissions emanating from the computer, thus preventing effective reception at reasonable distances."
(b) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	4:5-7 – "The EDP 12 includes an input/output (I/O) interface 18 for transferring data to and from the EDP through one or more serial or parallel data ports (not shown)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12." Figure 1.
(c) introducing noise into said measurement of said power consumption while processing said quantity; and	2:31-45 – "In a departure from the art, a signal masking technique is employed in which circuitry is coupled to the computer to radiate signals that fully emulate those radiated by the computer to be protected. The emulated signal emissions are synchronized with the computer signal emissions by a special control unit which receives timing instructions from the computer. The emulated signal emissions are synchronized to those of the computer with respect to time, amplitude and frequency. The emulated signals are also randomized or convoluted so that the composite signal emissions formed by the computer and the invention cannot be decoded to render meaningful data indicative of that being processed by the computer."

	2:67-3:3 – "A random sequence generator is included as part of the simulator to scramble the sequence of emulated signal emissions, rendering the composite signal meaningless for the purpose of discovering the original data." 3:65-68 – "According to the invention, the signal emission simulator 16 generates randomized signal emissions for the purpose of masking the signal emissions of the EDP 12." 4:45-48 – "Referring to FIGS. 1 and 2, the signal emission simulator 16 includes an emulation generator 22, a random sequence generator 24, a broad band RF amplifier 26 and a broad band antenna 28." 5:49-61 – "The amplifier 32 and antenna 28 in combination provide additional signal amplitude to the signal emissions of the generator 22." 5:62-6:7 – "The random sequence generator 24 of the simulator 16 is connected to the generator 22 by a line 52. The generator 24 convolutes or 'scrambles' the sequence of the signals generated by the generator 22, so that they would be meaningless if decoded. This is important since the generator 22 has just generated synchronous signals with the same character signatures as the EDP 12. The random sequence generator 24 comprises a circuit that operates as a noise source for introducing random or pseudo-random noise signals to the signals produced by the generator 22. The resulting signals are thereby convoluted in sequence, time, frequency and/or amplitude and thus garble any data that might have been decodable from the signals." 6:8-9 – "The generator 24 comprises a random sequence generator circuit." Figure 1.
(d) outputting said cryptographically processed quantity to a recipient thereof.	4:5-7 – "The EDP 12 includes an input/output (I/O) interface 18 for transferring data to and from the EDP through one or more serial or parallel data ports (not shown)." 4:59-5:6 – "The emulation generator 22 comprises the same circuit components as those used within the EDP 12 and the VDU 14 for processing digital or analog signals related to data that is to be protected from detection. The generator 22 includes an EDP circuit module 34, a VDU circuit module 36 and a drive circuit module 38. Lines 37 and 39 connect the module 36 and the module 38 to the module 34, respectively. The EDP circuit module comprises a printed circuit board substantially similar in components to the main PCB of the EDP 12, including a main memory 40, an I/O interface 42 and a

	central processing unit (CPU) 44. The components of the module 34 generate signal emissions which emulate those of the EDP 12." Figure 1.